

2. Second correction to text appearing on Page 3, bottom, of Amendment G:

In accordance with the present invention, an electronic signature program is described for the creation, monitoring, and verification of an electronic signature generated by the interaction between two computers, one a client and the other a server, for the signing of electronic data, such as documents, filings or transaction records without the need for an expensive and massive infrastructure of certification authorities and the complexities of installing and using digital certificates, [[-]]including cross-certifications, and/or without requiring hardware tablets and associated computer software. This system further is able to incorporate other existing technologies of prior art designed to authenticate users to a server computer and ones not yet available or existing.

3. Third correction to text appearing on Page 4, middle, of Amendment G:

Creation of the signature is depicted in figure 3. In the preferred embodiment, the server has captured the unique network element parameter of a signer, and where available, a credit card authorization number from a card processor. Where authentication on the basis of stored identity criteria, such as a digital certificate, username and password, or biometrics is involved, alphanumeric elements, appropriate symbols or abbreviations can be used to represent these. Other user identifier elements are known to those skilled in the art and may include a legacy application that has developed a user identifier system. Information from the user elements (no. 18) are combined with the date-time parameters of the server's system clock (no. 19) to create a signature transaction record, optionally with a Globally Unique Identifier (GUID) derived from the blend of the components through message digesting. (no. 20). Because time continuously progresses, each signature transaction that occurs sequentially at the signature server may be uniquely identifiable through the date and time of its creation. A unique network location, expressed as an IP address adds another element of uniqueness where two signature transaction records are created so closely in time as to have identical dates and time of creation. Since it is almost impossible for them to have originated simultaneously from the same network location, a unique network element parameter enables distinguishing